LOGÍSTICA • Con sus cyberlabs, la compañía ofrece a sus clientes las herramientas necesarias para reducir a mínimos el riesgo de ataque

SGS recomienda la "concienciación" como arma para encarar riesgos en ciberseguridad

ELENA GARCÍA
BARCELONA

La concienciación de todos los integrantes de empresas y organizaciones es clave para poder hacer frente a los riesgos en ciberseguridad. Ninguna entidad está libre de ser víctima de un ataque de este tipo, pero cuanto más concienciadas estén las personas que en ellas trabajan, mayor será la preparación de la empresa frente a dichos riesgos.

Este es uno de los puntos en los que más se incidió ayer, en la jornada sobre ciberseguridad que impartieron en la Asociación de Transitarios (ATEIA-OLTRA) de Barcelona, tres responsables del área de ciberseguridad de SGS: Susanna Caminals, business development manager de la compañía; Fabio Murillo, jefe de Secure Certification Management Systems & Training de la firma, y Juan Luis Romeo, team leader penetration testing.

Fabio Murillo fue muy claro al subrayar que "sin esta necesaria concienciación, sabemos que estamos rodeados de estos riesgos, pero pensamos que no nos va a pasar a nosotros", lo que hace más fácil para los hackers llevar a cabo el ataque y que este tenga éxito. Y, por supuesto, además de esta concienciación hay que contar con las herramientas adecuadas que pongan prácticamente imposible a los "malos" acceder a nuestros sistemas. Aunque "el riesgo cero no existe", reconoció Murillo.

Desde los cyberlabs, SGS apoya a sus clientes "de todo el mundo, de manera constante y estandarizada, 24 horas al día, 365 días al año" para evitar los ataques cibernéticos y, en caso de que estos se produzcan, minimizarlos

Los cyberlabs

Obstaculizar al máximo un ciberataque es en lo que trabajan en los cyberlabs de SGS. Tal y como explican desde la compañía, desde los cyberlabs SGS da soporte a sus clientes "de todo el mundo, de manera constante y estandarizada, 24 horas al día, 365 días al año" para evitar los ataques cibernéticos y, en caso de que estos se produzcan, minimizar las consecuencias.

La conectividad de productos o sistemas que antes estaban aislados presenta nuevas posibilidades de vulnerabilidad y desafíos relacionados con la ciberseguridad. "La experiencia ha demostrado que muchos de estos productos y sistemas, y sus componentes, a menudo tienen una protección inadecuada en caso de un ataque cibernético", precisan desde SGS.

Ante este nuevo escenario, el jefe de Secure Certification Management Systems & Training de SGS explicó que los cuatro pilares sobre los que SGS basa el sistema de seguridad que ofrece a sus clientes son: protección de los productos; seguridad de redes, comunicaciones y nube; seguridad de sistemas de gestión, servicios y certificaciones profesionales y, por último, integridad de datos.

En el caso de la seguridad de productos y sistemas, la protección se extiende tanto a componentes como a subcomponentes y a dispositivos, que van desde un teléfono móvil a un coche o un avión –de hecho, cualquier artilugio que esté conectado a internet–. "Poner atención en la seguridad de producto es vital", ya que muchas veces los ataques son posibles a través de los dispositivos más inesperados, señala Fabio Murillo.

Respecto a la seguridad de redes, la protección se centra en evaluaciones sobre redes, organizaciones e industrias, detectando y analizando todos los posibles accesos del sistema susceptibles de dar entrada a un ciberataque.

Garantías

En cuanto a la seguridad de sistemas de gestión, el jefe de Secure Certification Management Systems & Training explicó ante los socios de ATEIA-OLTRA Barcelona la importancia que tienen las actividades de certificación (como las ISO 27001 para la seguridad de la información o ISO22301 sobre sistemas de gestión de continuidad del negocio, por ejemplo) y capacitación en muchas organizaciones para dar al mercado "confianza en cómo tu entorno está creado en cuanto a ciberseguridad".

SGS es miembro tanto de la Asociación Público-Privada Europea (PPP) para la Ciberseguridad de la Comisión Europea (CE) como de la Organización Europea de Ciberseguridad (ESCO).

Susanna Caminals, business development manager de SGS; Juan Luis Romero, team leader penetration testing; y Fabio Murillo, jefe de Secure Certification Management Systems & Training. Foto EG.